IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW HAMPSHIRE
IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GMAIL ACCOUNT GOTVCALLS@GMAIL.COM, THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC
AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, Jill R. Laroe, being first duly sworn, hereby depose and state as follows:

1. I have been employed as a Special Agent of the FBI since 2002, and am currently assigned to Boston Division, Bedford Resident Agency working criminal matters, primarily white-collar criminal matters. During my time employed by the FBI, I have attended numerous trainings regarding constitutional law, cybercrime, money laundering, general investigative techniques and a variety of other types of criminal programs. I have been assigned to both criminal and terrorism programs and assisted in numerous white-collar/fraud/money laundering investigations, including as the lead investigator. Prior to joining the FBI, I was a member of the US Coast Guard where I also conducted law enforcement and search and rescue missions. I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).

2. Based on my training, personal experience, and participation in criminal investigations, I have become familiar with methods that individuals use to commit crimes, such as conspiracies against rights, financial crimes, to include money laundering, as well as crimes related to the obstruction of justice and destruction of evidence.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter but does include all information material to the probable cause inquiry.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of, inter alia, 18 U.S.C. § 1519 (destruction, alteration, or falsification of records in Federal investigations and bankruptcy) have been committed by the user of gotvcalls@gmail.com (the "SUBJECT ACCOUNT"). Pursuant to 18 U.S.C. § 1519, it is a crime when someone "knowingly alters, destroys … any record …with the intent to impede, obstruct, or influence the investigation or proper administration of any matter with the jurisdiction of any department or agency of the United States…."

5. Probable cause exists to search the information described in Attachment A for evidence of this crime, as described in Attachment B.

6. Agents with the FBI are investigating individuals who are or may be involved with robocalls (automated telephone calls which deliver a recorded message) that contained a message impersonating the voice of President Joe Biden, which provided misleading information about voting in the 2024 New Hampshire presidential primary. Among other individuals, the FBI is investigating Steve Kramer ("Kramer"), the user of the Subject Account, who was the primary person responsible for the creation and distribution of robocalls that contained the message impersonating President Joe Biden. In that message, the speaker, who was portrayed as President Biden, recommended that voters not vote in the NH Presidential Primary, which was being held on January 23, 2024, because their votes did not matter. The message was as follows: *"This coming Tuesday is the New Hampshire Presidential Preference Primary. Republicans have been trying to push nonpartisan and democratic voters to participate in their primary. What a bunch of malarkey. We know the value of voting democratic when our votes count. It's important that you save your vote for the November election. We'll need your help in electing Democrats up and down the ticket. Voting this Tuesday only enables the Republicans in their quest to elect Donald Trump again. Your vote makes a difference in November, not this Tuesday. If you would like to be removed from future calls, please press two now. Call {[ ]} to be removed from future calls."*

7. Steve Kramer has told investigators that he works as a political consultant and that he runs a company called "Get Out the Vote." Kramer said that he has decades of experience in the political field. On January 21, 2024, two days before the New Hampshire Primary, a telecommunications company retained by Kramer placed thousands of robocalls to New Hampshire voters using the fake President Biden voice message. Kramer has told investigators that he paid a person named Paul Carpenter ("Carpenter") to create the fake President Biden voice message. Kramer has essentially said that his goal was to bring attention to the dangers of Artificial Intelligence ("AI") in politics. Kramer denied that his purpose was to suppress votes. However, when asked whether he

believed that the people who received the robocall may have interpreted the call as that they should not go out to vote, Kramer said, "In the Republican primary."

8. On January 22, 2024, the New Hampshire Attorney General's Office issued a news release regarding the President Biden robocall and in that news release said that the office's Election Law Unit was investigating the incident.

9. Paul Carpenter has spoken to investigators and the news media about his role in the fake President Biden voice message. Carpenter told investigators that he is an acquaintance of Steve Kramer. Carpenter said that Kramer asked him to create the fake President Biden voice message that was used in the New Hampshire robocalls. Carpenter used commercially available AI software to create the message from a script that Kramer provided him. During his interview, Kramer advised that he began getting calls and requests from people to do something with AI after November's election. When Carpenter was interviewed, he was asked when he began to talk to Kramer about AI and advised that it was in September 2023 when he did an AI demonstration at a housewarming party Kramer was having in New Orleans. Carpenter also provided text messages to the FBI between himself and Kramer, and Venmo receipts for payment regarding creating AI recordings with Senator Lindsay Graham's voice for Kramer dating back to September 27, 2023.

10. Paul Carpenter has provided investigators with screenshots of some of his text messages with Steve Kramer. On January 22, 2023, Kramer sent Carpenter a text message that said, "Shhhhhhh." That was followed by a text message from Kramer that contained a link to a news article about the President Biden robocalls. That January 22, 2024, news article discussed the President Biden robocalls incident, and included the following statement: *"The New Hampshire attorney general's office says it is investigating what appears to be an "unlawful attempt" at voter suppression after NBC News reported on a robocall impersonating President Joe Biden telling recipients not to vote in Tuesday's presidential primary."* Carpenter responded to Kramer's texts with a text that said, "Gtfooh." "Gtfooh," is an abbreviation for the expression, "Get the fuck out of here." Kramer later told investigators that the "Shhhhhhh" message was sent to Carpenter because Kramer wanted a two-week period to pass so that he wasn't getting notoriety instead of the issue getting notoriety.

11. In a "Declaration" dated April 11, 2024, Paul Carpenter said that shortly after Steve Kramer sent him the text message and article, her and Kramer spoke on the phone. Over the phone, Kramer directed Carpenter to delete all emails and communications related to the creation of the Biden robocall. Carpenter said that Kramer assured him that because the call was "spoofed," it could not be traced back to either of them. Carpenter followed Kramer's directions and delated all his emails related to the creation of the recorded message from his Gmail account.

Carpenter stated that he no longer has the email from Kramer. However, Carpenter provided a screen shot from Carpenter's phone that showed several phone calls, voicemails and other text messages between Carpenter and Kramer occurring on January 22, 2024.

12. On January 31, 2024, the Federal Communications Commission ("FCC"), issued a press release concerning AI voice-generated robocalls. On February 6, 2024, the FCC issued another news release specifically about the fake President Biden robocalls and enforcement actions that were being taken in connection with those calls.

13. When investigators spoke to Steve Kramer on February 29, 2024, and asked him if he asked Paul Carpenter to delete the emails and erase messages that the two of them had together, Kramer twice said, "I don't think so." Kramer then stated that maybe he asked Carpenter to hold back because essentially Kramer wanted to wait until after the South Carolina primary to go public. Based on Kramer's equivocal answer as to whether he asked Carpenter to destroy records of their communications and the fact that Carpenter said that Kramer asked him to destroy their communications with one another about the President Biden robocalls, there is probable cause to believe that Kramer also deleted and erased his communications with Carpenter about the President Biden robocalls. Moreover, given that Kramer told Carpenter to delete emails in the context of keeping quiet about the President Biden robocalls after sharing an article with Carpenter regarding the New Hampshire Attorney General's investigation, there is probable cause to believe that Kramer deleted his communications with Carpenter, in part, in contemplation of a potential federal investigation. Investigators have received emails between Kramer and Carpenter. However, it is unknown if investigators have all the emails between them since Carpenter said he deleted communications at Kramer's request.

14. Paul Carpenter has said that he has mental health, substance abuse, and gambling issues. In February 2024, Carpenter may have committed a crime when he reportedly impersonated another person online and convinced the victim to send him approximately $8,000 in crypto currency. Despite Carpenter's issues, much of what he has told investigators and others has been verified by Steve Kramer and text messages between Kramer and Carpenter. In addition, Carpenter has been cooperative with investigators and not declined any of their requests in connection with this investigation.

15. Investigators have learned that Paul Carpenter's email is mentallyhyp2012@gmail.com, and that Steve Kramer's email is

gotvcalls@gmail.com. Both email addresses are Gmail accounts.

16. I believe that a search of Steve Kramer's Gmail account may yield evidence of deleted communications between Kramer and Paul Carpenter.

17. The government submitted a preservation letter to Google for the SUBJECT ACCOUNT on or about February 23, 2024.

18. In general, an email that is sent to a Gmail subscriber is stored in the subscriber's "mailbox" on Gmail servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Gmail servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Gmail's servers for a certain period of time.

19. In my training and experience, I have learned that Gmail provides a variety of online services, including electronic mail access, to the public. Gmail allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Gmail. During the registration process, Gmail asks subscribers to provide basic personal information. Therefore, the computers of Gmail are likely to contain stored electronic communications (including retrieved and unretrieved email for Gmail subscribers) and information concerning subscribers and their use of Gmail services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. A Gmail subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Gmail. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists,

email in the account, and attachments to emails, including pictures and files.

21. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

22. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

23. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support

services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the government to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement). For these reasons, I am seeking copies of Steve Kramer's emails and other information

associated with the SUBJECT ACCOUNT from September 1, 2023, through March 1, 2024.

25. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Gmail to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate that is described in Section II of Attachment B.

CONCLUSION

26. Based on the foregoing, I request that the Court issue the proposed search warrant.

27. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

28. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court "a district court of the United States ... that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

29. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss

an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

For the reasons outlined above, I believe there is probable cause to support a search warrant authorizing the search of Steve Kramer's Gmail account (gotvcalls@gmail.com), which may provide evidence of a violation of 18 U.S.C. § 1519 (destruction, alteration, or falsification of records in Federal investigations and bankruptcy).

/s/ Jill R. Laroe
Jill R. Laroe
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. P. 41 and affirmed under oath the contents of this affidavit and application.

Date: **Jun 5, 2024**

Time: **2:01 PM**

Talesha L. Saint-Marc
United States Magistrate Judge

ATTACHMENT A

A: Property to Be Searched

This warrant applies to information associated with gotvcalls@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered in Mountain View, California ("Gmail").

ATTACHMENT B

B: Particular Things to be Seized.

Information to be Disclosed by Gmail (the "Provider") To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on February 23, 2024 (reference #53740544), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A: a. The contents of all emails associated with the account from September 1, 2023, through March 1, 2024, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email; b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number); c. The types of service utilized; d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and 2. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government: All information

described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1519 (Destruction, alteration, or falsification of records in Federal investigations and bankruptcy) involving Steve Kramer, in or about and between September 1, 2023 through March 1, 2024, including, for the account or identifier listed on Attachment A, information pertaining to the following matters: (a) Evidence relating to the deletion of emails and communications regarding the creation, formulation and distribution of materials intended to impede and/or interfere with the voting rights of American citizens, and/or discussions thereof; (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner; (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation; (d) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s) and other platforms used by co-conspirators to communicate; and (e) The identity of the person(s) who communicated with the user of the account about matters relating to deletion of emails and communications regarding the creation, formulation and distribution of materials intended to impede and/or interfere with the voting rights of American citizens, and/or discussions thereof, including records that help reveal their whereabouts. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and for instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.